REMARKS

Claims 2, 4-7 and 9-20 are pending. By this Amendment, claims 18 and 19 have been amended to correct typographical errors, but not for any reasons with regard to the patentability of the recited subject matter.

Rejection under 35 U.S.C. § 112, First Paragraph

The Office Action rejected claims 18-20 under 35 U.S.C. § 112, first paragraph ("112(1)") because the specification allegedly does not include support for the claimed "decrypt[ing] … the encrypted IMEI received from the storage support module using a second key." (Office Action, pp. 4-5.) Applicant respectfully traverses this rejection.

To satisfy the written description requirement under § 112(1), a specification must describe the claimed subject matter in sufficient detail that one skilled in the art could reasonably conclude that the inventor had possession of the claimed invention. However, the specification is **not required** to disclose, and **preferably omits** what is well known in the art. *In re Buchner*, 929 F.2d 660, 661, 18 USPQ2d 1331, 1332 (Fed. Cir. 1991); *Hybritech, Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1384, 231 USPQ 81, 94 (Fed. Cir. 1986), *cert. denied*, 480 U.S. 947 (1987); and *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1463, 221 USPQ 481, 489 (Fed. Cir. 1984); MPEP § 2164.01. (Emphasis added.)

Applicant's Specification supports the claimed "encrypt[ing], … the IMEI using the first key," and "decrypt[ing] … the encrypted IMEI received from the storage support module using the second key." For instance, the Specification states:

> In order to secure the channel 6 and to perform any necessary authentications between the storage support 2 and the module 31, the support 2 and/or the module can **store encryption keys** adapted to the desired type of encryption or authentication. The types of **encryption** …

> to be used are already known. It is possible, in particular, to consider using session keys or static keys.
>
> The integrity of the IMEI can be protected by **a cryptographic calculation, which will be sent over the secure channel 6** to the secure module 31.

(Specification, p. 7, ll. 5-15, emphasis added.) Hence, based on at least the Specification's disclosure of "encryption" and "keys," it provides explicit support for the claimed "encrypting," "decrypting," "first key" and "second key."

The Examiner apparently believes that the Specification does not support the claimed "decrypting" and "second key" because these *exact* terms are not used in the Specification. **However, "there is no *in haec verba* requirement" and "newly added claim limitations may be supported in the specification through express, implicit, or inherent disclosure."** M.P.E.P. § 2163(I)(B). (Emphasis added.)

The Specification's disclosure of "encryption" encompasses both "encrypting" and "decrypting." While the Specification does not detail the encryption process, Applicant's specification states "[t]ypes of encryption … to be used are already know." Because encryption techniques are well known, § 112(1) does not require that the specification to provide details of performing known "encryption" processes using the "encryption keys" to encrypt and "decrypt" the IMEI from a "cryptographic calculation."

One of ordinary skill in the art of secure transmissions would understand Applicant's disclosure of "encryption" to support both "encrypting" and "decrypting." The term "encryption" is generally considered to include a transmitter that performs encrypting and a receiver that performs **decrypting**. For example, the *McGraw-Hill Dictionary of Scientific and Technical Terms* defines "encryption" as "**coding** of a clear text message by a transmitting unit so as to prevent unauthorized eavesdropping along the transmission line; the receiving unit uses the same algorithm as the transmitting unit to **decode** the incoming

message." (*McGraw-Hill Dictionary of Scientific and Technical Terms*, retrieved December 14, 2010, from http://www.answers.com/topic/encryption, emphasis added.)

Applicant's Specification describes storing encryption keys and using encryption to send an IMEI 21 securely between a storage support 2 and a secure electronic module 31 as a "cryptographic calculation." (Specification, p. 7, ll. 5-15.) Furthermore, the Specification states that the secure electronic module 31 transmits the IMEI 21 to a server 7. (*Id.* at p. 8, ll. 8-11.) This could not occur unless the secure electronic module 31 had decrypted the received IMEI 21. Thus, in the context of the specification, an artisan having ordinary knowledge of secure transmission techniques would understand the disclosed "encryption" to describe both encrypting and decrypting using the disclosed "encryption keys."

For all the reasons above, the subject matter recited in claims 18 satisfies the requirements of § 112(1). Claims 19 and 20 also satisfy § 112(1) for the same reasons. Applicant, therefore, respectfully requests that the rejection of claims 18-20 under § 112 be reconsidered and withdrawn.

Rejection under 35 U.S.C. 103

The combination of U.S. Patent Publication No. 2004/0043792 by *Simmons* and U.K. Patent Application No. GB2355892 by *Portalier et al.* ("*Portalier*") cannot support a rejection of the pending claims under 35 U.S.C. § 103(a) because the references do not establish that all the features recited in the claims were known in the art at the time of the invention. (*See KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385, 1395 (2007); M.P.E.P. § 2143.02.)

First, *Simmons* and *Portalier* say nothing with regard to "establish[ing] … in the event the secure electronic module determines that the storage support module is authentic, a secure

communication channel." The Applicant previously argued that the cited references failed to disclose this feature in the Amendment dated July 29, 2010. The Office Action acknowledged this argument. (Office Action, p. 2.) However, the Office Action does not particularly respond to the argument or cite any evidence that might establish the claim feature is disclosed. (*Id.* at pp. 2-4 and p. 5, l. 25 to p. 6, l. 2.) Accordingly, the Office Action does not provide sufficient evidence to support a rejection of claim 18 under § 103 for at least this reason.

In fact, *Simmons* merely states that a SIM card 20 generates a challenge used to verify that a terminal device is compatible with pre-paid operation. However, this verification cannot be considered to teach or suggest, "establishing … a secure communication channel," as recited in claim 18. Hence, *Simmons* cannot be considered to teach or suggest the above-noted feature of claim 18. *Portalier* also does not teach or suggest this claim feature either, and the Office Action does not assert that *Portalier* makes any such disclosure. Thus, *Simmons* and *Portalier* cannot support a rejection of claim 18 under § 103 for this reason as well.

Second, *Simmons* and *Portalier* do not disclose or suggest, "encrypt[ing], by the storage support module, the IMEI using [a] first key," "decrypt[ing], by the secure electronic device, the encrypted IMEI received from the storage support module using [a] second key" and "enabl[ing], by the secure electronic module, the handset to access the communication network in the event the secure electronic module determines that the decrypted IMEI received from the storage support module is authentic," as recited in claim 18. The Examiner apparently did not give the claimed "encrypt[ing]… the IMEI using the first key" and "decrypt[ing] the encrypted IMEI received from the storage support module using the second key" patentable weight because he does not believe these features are sufficiently supported

by the specification. (Office Action, p. 6.) However, for the reasons set given above, the rejection of claim 18 under § 112(1) is improper and the claimed "encrypting" and "decrypting" are supported by Applicant's specification. Thus, these features must be given patentable weight.

The Examiner appears to recognize that the cited references do not disclose or suggest, "encrypt[ing]… the IMEI **using the first key**," and "decrypt[ing], by the secure electronic device, the encrypted IMEI **using the second key**." (Emphasis added.) Actually, *Simmons* and *Portalier* are silent with regard to the claimed "keys." Moreover, because the references do not disclose or suggest the claimed "encrypting and decrypting," they also cannot be considered to teach or suggest, "enabl[ing] … in the event the secure electronic module determines that **the decrypted IMEI** … is authentic." (Emphasis added.) Because the applied references do not disclose or suggest the above-noted features of claim 18, the references cannot support a rejection of claim 18 under § 103. Claim 18 is, therefore, allowable over *Simmons* and *Portalier*.

Third, the Office Action concedes that *Simmons* does not disclose "access, by the handset, the communication network using the authenticated IMEI, wherein the network grants access to the handset without further authentication of the authenticated IMEI," as recited in claim 18 and, instead, alleges that *Portalier* discloses this claim feature. (Office Action, pp. 6, *citing Portalier*, p. 7, l. 20 to p. 8, l. 13.) On the contrary, *Portalier* simply permits **the use of a mobile telephone** in the case a code matches. (*Portalier*, p. 8, ll. 3-7.) *Portalier* does not, however, say anything with regard to a "network **grant[ing] access** to the handset without further authentication of the authenticated IMEI," as recited in claim 18. Since *Simmons* and *Portalier* both fail to disclose or suggest this feature, these references cannot support a rejection of claim 18 under § 103. (Emphasis added.)

Furthermore, nothing in the cited references, when taken individually or in combination, teach or suggest the claimed combination of features **as a whole**. *See Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983); *Schenck v. Nortron Cor*p., 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983); M.P.E.P. § 2142.02. That is, *Simmons* and *Portalier* do not disclose or suggest the claimed combination of features, including "authenticat[ing] the secure electronic module," "establish[ing] establish, in the event the secure electronic module determines that the storage support module is authentic, a secure communication channel," "encrypt[ing] … the IMEI," "transmit[ing, via the secure communication channel, the encrypted IMEI," "decrypt[ing] … the encrypted IMEI" and "enable[ing], by the secure electronic module, the handset to access the communication network in the event the secure electronic module determines that the decrypted IMEI received from the storage support module is authentic" the cited references also cannot be considered to disclose "access[ing], by the handset, the communication network using the authenticated IMEI… **without further authentication of the authenticated IMEI**," as recited in claim 18. (Emphasis added.) Accordingly, *Simmons* and *Portalier* cannot support a rejection of claim 18 for this additional reason.

For all the reasons above, claim 18 is allowable over *Simmons* and *Portalier*. Applicant, therefore, request that the rejection of claim 18 be reconsidered and withdrawn.

Claims 19 and 20 recite subject matter similar to that in claim 18. Accordingly, claims 19 and 20 are also allowable over *Simmons* and *Portalier* for the same reasons as claim 18. Dependent claims 2, 4-7 and 9-17 are allowable at least due their dependence from claims 18 and 19, in addition to reciting other allowable subject matter.

Conclusion

For the reasons set forth above, Applicant respectfully requests allowance of the pending claims. If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: December 14, 2010

By: /Steven Ashburn/
Steven Ashburn
Registration No. 56,636

Customer No. 21839
703 836 6620